What is claimed is:

1. A method of detecting intrusion attempts by an imposter in a communications network, said method comprising the steps of:

at a victim node, determining that a received packet comprises an address corresponding to said victim node; and in response thereto,

transmitting an emergency packet;

at a destination node, receiving said emergency packet and, in response thereto, generating an intrusion attempt indication;

at a destination node, detecting a carrier signal not followed by receipt of said emergency packet, and in response thereto transmitting an emergency packet request; and

at said victim node, resending said emergency packet in response to receipt of said emergency packet request.

2. The method according to claim 1, wherein said emergency packet is transmitted within an emergency window following the end of the received packet.

3. The method according to claim 1, wherein receipt of said carrier signal is checked during an emergency window following the end of the received packet.

4. The method according to claim 1, wherein said emergency packet request is transmitted during an acknowledgement window that follows an emergency window.

5. The method according to claim 1, further comprising the steps of:

repeatedly transmitting said emergency packet request a predefined number of times if said carrier signal is detected without receipt of an emergency packet; and

generating an intrusion attempt indication upon failure to receive said emergency packet.

6. The method according to claim 5, wherein said predefined number of times equals two.

7. The method according to claim 1, further comprising the step of sending said received packet along with said intrusion attempt indication to a host.

8. The method according to claim 1, further comprising the step of determining whether said victim node is also a destination node and if so, generating said intrusion attempt indication without transmitting said emergency packet.

9. The method according to claim 1, further comprising the step of continually resending said emergency packet with random backoff times until receiving an indication of receipt by the destination node.

10. The method according to claim 1, further comprising the step of said victim node transmitting a regular packet to a Network Administrator entity indicating said imposter node used its address.

11. The method according to claim 1, wherein said method is implemented in an Application Specific Integrated Circuit (ASIC).

12. The method according to claim 1, wherein said method is implemented in a Field Programmable Gate Array (FPGA).

13. A method for use in a victim node of detecting intrusion attempts by an imposter in a communications network, said method comprising the steps of:

determining that a received packet comprises an address corresponding to said victim node; and in response thereto,

transmitting to a destination node an emergency packet; and

resending said emergency packet in response to receipt of an emergency packet request transmitted from said destination node.

14. The method according to claim 13, wherein said emergency packet is transmitted within an emergency window following the end of the received packet.

15. The method according to claim 13, further comprising the step of determining whether said victim node is also a destination node and if so, generating an intrusion attempt indication without transmitting said emergency packet.

16. The method according to claim 13, further comprising the step of continually resending said emergency packet with random backoff times until receiving an indication of receipt by the destination node.

17. The method according to claim 13, wherein said method is implemented in an Application Specific Integrated Circuit (ASIC).

18. The method according to claim 13, wherein said method is implemented in a Field Programmable Gate Array (FPGA).

19. A method for use in a destination node of detecting intrusion attempts by an imposter in a communications network, said method comprising the steps of:

receiving a received packet transmitted over said communications network;

listening during an emergency window for the presence of carrier signal;

if carrier signal is detected during said emergency window and an emergency packet is received subsequent thereto, generating an intrusion attempt indication; and

if carrier signal is detected during said emergency window and no emergency packet is received subsequent thereto, transmitting an emergency packet request and repeating said step of listening.

20. The method according to claim 19, wherein receipt of said carrier signal is checked during said emergency window following the end of the received packet.

21. The method according to claim 19, wherein said emergency packet request is transmitted during an acknowledgement window following said emergency window.

22. The method according to claim 19, further comprising the steps of:

repeatedly transmitting said emergency packet request a predefined number of times if said carrier signal is detected without receipt of an emergency packet; and

generating an intrusion attempt indication upon failure to receive said emergency packet.

23. The method according to claim 22, wherein said predefined number of times equals two.

24. The method according to claim 19, further comprising the step of sending said received packet along with said intrusion attempt indication to a host.

25. The method according to claim 19, further comprising the step of continually resending said emergency packet with random backoff times until receiving an indication of receipt by the destination node.

26. The method according to claim 19, wherein said method is implemented in an Application Specific Integrated Circuit (ASIC).

27. The method according to claim 19, wherein said method is implemented in a Field Programmable Gate Array (FPGA).

28. An Application Specific Integrated Circuit (ASIC) for use in a node for detecting intrusion attempts by an imposter in a communications network, said ASIC comprising:

means for determining that a received packet comprises an address corresponding to said node;

means for transmitting an emergency packet following the end of said received packet if said node determines said received packet comprises the address of itself;

means for receiving said emergency packet and generating an intrusion attempt indication, in response thereto;

means for detecting a carrier signal without subsequent receipt of said emergency packet and transmitting an emergency packet request, in response thereto; and

means for resending said emergency packet in response to receipt of said emergency packet request.

29. The ASIC according to claim 28, wherein said emergency packet is transmitted within an emergency window following the end of the received packet.

30. The ASIC according to claim 28, wherein it is checked for receipt of said carrier signal during an emergency window following the end of the received packet.

31. The ASIC according to claim 28, wherein said emergency packet request is transmitted during an acknowledgement window following an emergency window.

32. The ASIC according to claim 28, further comprising means adapted to:

repeatedly transmit said emergency packet request a predefined number of times if said carrier signal is detected without receipt of an emergency packet; and

generate an intrusion attempt indication upon failure to receive said emergency packet.

33. The ASIC according to claim 32, wherein said predefined number of times equals two.

34. The ASIC according to claim 28, further comprising means for sending said received packet along with said intrusion attempt indication to a host.

35. The ASIC according to claim 28, further comprising means for determining whether said node is both a victim and destination node and if so, generating said intrusion attempt indication without transmitting said emergency packet.

36. A communications station for transmitting and receiving signals to and from other stations connected over a shared communications media based network, comprising:

a coupling circuit for generating a receive signal received over said network and for outputting a transmit signal onto said network;

a transmitter adapted to modulate a synchronization sequence and data to be transmitted in accordance with a modulation scheme so as to generate said transmit signal therefrom, said synchronization sequence comprising a plurality of symbols wherein each symbol is separated by a time delay in accordance with a predetermined synchronization sequence time delay template;

a receiver adapted to demodulate said receive signal in accordance with said modulation scheme so as to generate a receive data signal therefrom;

a media access control (MAC) circuit adapted to interface an application processor to said shared communications media, said MAC circuit comprising:

means for determining that a received packet comprises an address corresponding to said node;

means for transmitting an emergency packet following the end of said received packet if said node determines said received packet comprises the address of itself;

means for receiving said emergency packet and generating an intrusion attempt indication, in response thereto;

means for detecting a carrier signal without subsequent receipt of said emergency packet and transmitting an emergency packet request, in response thereto;

means for resending said emergency packet in response to receipt of said emergency packet request; and

said application processor adapted to control the operation of said transmitter, receiver and MAC and to provide an interface between said MAC and an external host.

37. The communications station according to claim 36, wherein said modulation scheme comprises code shift keying (CSK) modulation.

38. The communications station according to claim 36, wherein said emergency packet is transmitted within an emergency window following the end of the received packet.

39. The communications station according to claim 36, wherein detection of said carrier signal occurs during an emergency window following the end of the received packet.

40. The communications station according to claim 36, wherein said emergency packet request is transmitted during an acknowledgement window following an emergency window.

41. The communications station according to claim 36, further comprising:

means for repeatedly transmitting said emergency packet request a predefined number of times if said carrier signal is detected without receipt of an emergency packet; and

means for generating an intrusion attempt indication upon failure to receive said emergency packet.

42. The communications station according to claim 41, wherein said predefined number of times equals two.

43. The communications station according to claim 36, further comprising means for sending said received packet along with said intrusion attempt indication to a host.

44. The communications station according to claim 36, further comprising means for determining whether said node is both a victim and destination node and if so, generating said intrusion attempt indication without transmitting said emergency packet.

45. The communications station according to claim 36, wherein said MAC is implemented in an Application Specific Integrated Circuit (ASIC).

46. The communications station according to claim 36, wherein said MAC is implemented in a Field Programmable Gate Array (FPGA).

47. A computer program product for use in communications station, said computer program product comprising:

a computer useable medium having computer readable program code means embodied in said medium for detecting intrusion attempts by an imposter in a communications network, said computer program product comprising:

computer readable program code means for determining that a received packet comprises an address corresponding to said node;

computer readable program code means for transmitting an emergency packet following the end of said received packet if said node determines said received packet comprises the address of itself;

computer readable program code means for receiving said emergency packet and generating an intrusion attempt indication, in response thereto;

computer readable program code means for detecting a carrier signal without subsequent receipt of said emergency packet and transmitting an emergency packet request, in response thereto; and

computer readable program code means for resending said emergency packet in response to receipt of said emergency packet request.